ICS 45.020
CCS L70

团 体 标 准

T/CAMET XXXX—XXXX

城市轨道交通 互联网协议第六版（IPv6+）技术要求

Urban rail transit—Technical requirements of Internet Protocol version 6 Plus(IPv6+)

（工作组讨论稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国城市轨道交通协会 发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国城市轨道交通协会信息化专业委员会提出。

本文件由中国城市轨道交通协会标准化技术委员会归口。

本文件起草单位：深圳市地铁集团有限公司、北京市地铁运营有限公司、上海申通地铁集团有限公司、广州地铁集团有限公司、宁波市轨道交通集团有限公司、无锡地铁集团有限公司、重庆市轨道交通（集团）有限公司、南昌轨道交通集团有限公司、佛山市地铁运营有限公司、哈尔滨地铁集团有限公司、济南轨道交通集团有限公司，深圳信息通信研究院、华为技术有限公司、中国移动通信集团广东有限公司深圳分公司、深圳市市政设计研究院有限公司、中国铁路设计集团有限公司、南京亚信智网科技有限公司、深信服科技股份有限公司、深圳市联软科技股份有限公司、北京连星科技有限公司。

本文件主要起草人：黄一格、鲁青松、侯铁、刘晓溪、岳栋、李广、潘健英、张昊、杨青、陈伟玮、赵宸、张攀、林子杰、毕荣梁、敖日格勒、莫尚平、曹炎杰、黄丹妮、马凯、宋华、郑鹏、马涛、周宇航、徐佑民、赵阳、黄新、刘小飞、贺佐辉、袁伟、赵浩博、赵甘临、汤宇为、张立东、沈琦、林德辉、肖华平、许玲、汪可可、管剑波、戴浩峰、晁睿、刘铮、鄢光绪、喻若、彭阳衍、胡华、冼志威、丁晶、张亦弛、娄飞鹏、柏成勇。

城市轨道交通 互联网协议第六版（IPv6+）技术要求

1 范围

本文件规定了城市轨道交通 互联网协议第六版（IPv6+）技术要求，包括总体原则、地址规划与管理、基础平台、网络、安全、应用、终端。

本文件适用于城市轨道交通的地铁系统、市域快轨系统、轻轨系统、中低速磁浮系统、跨座式单轨系统、悬挂式单轨系统、自导向轨道系统、有轨电车系统、导轨式胶轮系统、电子导向胶轮系统等多种运输制式，作为指导城市轨道交通管理单位、参建单位、第三方服务提供方开展IPv6+应用的技术要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

YD/T 3975 5G网络切片 基于IP承载的端到端切片对接技术要求

T/CAMET 11001 智慧城市轨道交通 信息技术架构及网络安全规范

T/CAMET 11002 城市轨道交通云平台构建技术规范

T/CAMET 11004 城市轨道交通云平台网络架构技术规范

T/CAMET 11005 城市轨道交通云平台网络安全技术规范

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

安全生产网 safety production network

用于承载城市轨道交通运营生产类面向一线生产及调度人员服务的应用系统的计算机网络。

3.1.2

内部管理网 internal management network

用于承载城市轨道交通运营管理、企业管理、建设管理、资源管理等面向企业内部用户服务的应用系统的计算机网络。

3.1.3

外部服务网 external service network

用于承载城市轨道交通乘客服务类等面向外部或公众用户服务应用系统的计算机网络。

3.1.4

城域网 wide area network

一种IEEE许可的支持城市区域高速传输的网络，覆盖一个城市的地理范围，用来将同一区域内的多个局域网互联起来的中等范围的互联网络。

3.1.5

局域网 local area network

企业或者站点的内部网络，由局部地区形成的一个区域网络，其特点就是分布地区范围有限。局域网络的规模可小可大，小到只有十几人的单台交换机或无线AP，大到上万人的涉及数千个设备。

3.1.6

互联网协议第六版升级 internet protocol version 6 plus

互联网协议第六版升级简称IPv6+，是基于IPv6下一代互联网的全面升级，包括以SRv6、网络切片、iFIT、BIERv6、APN6等为代表的协议创新，还包括以网络分析、网络自愈、自动调优等为代表的网络智能化技术创新。

3.1.7

基于 IPv6 转发平面的段路由 segment routing ipv6

基于IPv6转发平面的段路由，基于源路由理念而设计的在网络上转发IPv6数据包的一种方法。

3.1.8

网络切片 network slicing

在一个物理网络上构建多个端到端的、虚拟的、隔离的、按需定制的专用网络，实现一网多用，以满足不同系统对网络能力的不同要求（时延、带宽、连接数、可靠性等）。

3.1.9

随流检测 in-situ flow information telemetry

直接对业务报文进行端到端测量，从而得到网络的真实丢包率、时延等性能指标的检测方式，具有部署方便、统计精度高等突出优点。

3.1.10

应用感知的 IPv6 网络，APN6 application-aware ipv6 networking

利用IPv6扩展报文头空间，将应用信息（APN Attribute）携带进入网络，包括应用标识信息（APN ID）和应用需求参数信息（APN Parameters），进而为应用和用户提供精细的网络服务和精准的网络运维。

3.1.11

客户端/服务器架构 client/server structure

一种通常由一台或多台服务器以及大量的客户机组成网络软件运行形式。服务器配备大容量存储器并安装数据库系统，用于数据的存放和数据检索。客户端安装专用的软件，负责数据的输入、运算和输出。

3.1.12

浏览器/服务器架构 browser/server structure

对客户端/服务器架构的一种变化或者改进的结构，在该结构下，用户工作界面是通过Web浏览器来实现，主要事务逻辑在服务器端实现，而前端浏览器只实现极少部分事务逻辑。

3.1.13

遥测技术 telemetry

新一代从设备上远程高速采集数据的网络监控技术，设备通过“推模式（Push Mode）”周期性地主动向采集器上送设备信息，提供更实时、更高速、更精确的网络监控功能。

3.1.14

灵活以太 flexible ethernet

实现业务隔离承载和网络分片的一种接口技术。基于时隙调度将一个物理以太网端口划分为多个以太网弹性硬管道，使得网络具备类似于TDM（时分复用）独占时隙、隔离性好的特性，又具备以太网统计复用、网络效率高的双重特点，实现同一分片内业务统计复用，分片之间业务互不影响。

3.1.15

灵活子通道 flex channel

基于HQoS机制分配独立的队列和带宽资源的业务通道。Flex-channel之间带宽严格隔离，提供了一种灵活和细粒度的接口资源预留方式。

3.1.16

全球单播地址　global unicast address

全球单播地址GUA：2000::/3。在RFC3587中定义，全球唯一、可Internet路由，类似于IPv4公网地址。

3.1.17

唯一本地地址 unicast local address

唯一本地地址（ULA）：fc00::/7。在RFC4193中定义，站点内有效，类似于IPv4的私网地址，用于大型网络的内部通信。

3.1.18

链路本地地址 link-local address

链路本地地址（LLA）：fe80:10，仅限于本地链路范围内使用。节点可以自动生成，用于相邻节点之间使用，如邻居发现、无状态地址配置等应用，实现即插即用功能。

3.1.19

IPv6流标签 ipv6 flow label

IPv6的路由技术之一，用于标识特定流第一个报文头部所描述的选路和处理过程，以及网络设备所确定的选路和处理策略。

3.1.20

IPv6微分段 ipv6 micro-segmentation

微分段是一种细粒度的安全策略。微分段基于对报文进行分组后的组标识，将数据中心网络细分为更小粒度的多个安全区域，实施网络隔离和访问控制策略，从而增强网络的安全性。IPv6微分段是指在网络中使用IPv6协议进行微分段配置的一种技术。

3.2　缩略语

下列缩略语适用于本文件。

APN6：应用感知的IPv6网络（Application-aware IPv6 Networking）
BAS：环境与设备监控系统（Building Automatic System）
BGP4+：IPv6边界网关协议（Border Gateway Protocol for IPv6）
BIM：建筑信息模型（Building Information Modeling）
DHCPv6：动态主机配置协议版本6（Dynamic Host Configuration Protocol version 6）
DNS：域名服务（Domain Name Service）
EBGP：外部边界网关协议（External Border Gateway Protocol）
FIBv6：IPv6转发表（IPv6 Forwarding Information Table）
GUA：全球单播地址（Global Unicast Address）
ICMPv6：因特网控制报文协议第6版（Internet Control Message Protocol version 6）
iFIT：随流检测技术（in-situ Flow Information Telemetry）
IPAM：IP地址管理（IP Address Management）
IPv4：互联网协议第四版（Internet Protocol version 4）

IPv6：互联网协议第六版（Internet Protocol version 6）
IPv6+：基于IPv6下一代互联网升级
ISP：互联网服务提供商（Internet Service Provider）
IS-IS：中间系统到中间系统协议（Intermediate System to Intermediate System）
LLA：链路本地地址（Link-Local Address）
MLD：多播接收方发现协议（Multicast Listener Discovery）
MP-BGP：BGP多协议扩展（Multiprotocol Extensions for BGP）
MPLS：多协议标签交换（Multiprotocol Label Switching）
NAT：网络地址转换（Network Address Translation）
NAT66：IPv6网络地址转换（Network Address Translation IPv6 to IPv6）
ND：邻居发现（Neighbor Discovery）
PSCADA： 电力监控系统（Power Supervisory Control and Data Acquisition system）
QoS：服务质量（Quality of Service）
SDN：软件定义网络（Software Defined Network）
SLAAC：无状态地址自动配置（Stateless address autoconfiguration）
SRv6：基于IPv6的段路由（Segment Routing over IPv6）
ULA：唯一本地地址（Unicast Local Address）
VPN：虚拟专用网络（Virtual Private Network）
4G：第四代移动通信系统（4th Generation）
5G：第五代移动通信系统（5th Generation）
6vPE：IPv6虚拟专用网络提供商边界（IPv6 Virtual Provider Edge）

4 总体原则

4.1 实用性原则

系统软硬件采用国内通用的、成熟的软硬件产品，保证系统功能的高效稳定。

4.2 稳定性原则

采用成熟稳定的技术和简单易行的方法进行业务的升级改造，保证各项服务的不间断性，既支撑IPv6应用部署及用户访问，又保证IPv4网络稳定安全运行。

4.3 节约投资原则

轨道交通目前会长期存在IPv4单栈、IPv4/IPv6双栈、IPv6单栈三种形态，考虑三种场景兼容。同时考虑最终建设目标为IPv6单栈，尽量避免二次改造。

4.4 地址规划原则

IPv6地址规划遵照下列原则：

a) 语义化：地址可读性强，能够包含所属区域、用途等信息，便于识别用户所在区域及用途。
b) 聚合性：IPv6 地址规划宜考虑路由发布需求,增强路由聚合能力。对于跨自治域广播的路由、跨区域广播的路由、网内广播的路由应有明确的不同前缀长度限定，减少地址碎片，减小路由表。
c) 连续可扩展:宜考虑安全生产、内部管理和外部服务等网络区域和各二三级单位地址的连续性。对某些具有安全等特殊要求的业务网络宜考虑为其规划一个连续的地址段。
d) 可管控：宜将 IPv6 地址规划为一定的层次结构，简洁直观，满足对业务的优先级、访问控制等管理要求，方便进行网络管理和运维。

4.5 互通性原则

向IPv6迁移过程中，要考虑分级建设、分层管理的模式，支持上下级网络、同一级网络内部不同设备之间改造进度不一致的情况。

4.6 安全原则

关注IPv6涉及的安全风险，做好相应安全防护策略和安全技术部署，最大限度保障网络与信息资源安全，保障系统稳定可靠运行。

5 地址规划与管理

5.1 一般要求

地址规划与管理总体应满足下列要求：

a) 安全生产网和内部管理网优先采用 IPv6 ULA 地址规划 ，需要与互联网或其他外部网络进行IPv6 通信时，使用网络前缀转换技术（NPTv6）将 ULA 转为对应 GUA，公有云应用采用 IPv6 GUA 地址直接提供访问；

b) IPv6 GUA 地址申请前缀最终获批可能为 32 位、48 位、52 位、56 位等地址范围，因此在地址规划时，预留一定地址位，方便后续申请替换。

5.2 地址结构

本文件采用IPv6 ULA地址段FC00:0::/32来规划示例，其中可分配的地址范围为：FC00::/32，应采用结构化编址方式进行地址规划设计。地址结构应满足下列要求。

a) IPv6地址规划宜按4位，16种取值的倍数进行地址域分配，宜根据类型、机构、地域、部门域、专业域和主机域进行划分，主机域按后65～128位规划，作为主机地址使用。IPv6地址结构宜参照表1。

表 1 IPv6 地址结构

固定前缀	类型域	机构域	地域/部门域	专业域	预留域	主机域
FC00::/32	X	Y	Z	W	VVV	0000:0000:0000:0000
1-32 位	33-36 位	37-40 位	41-48 位	48-51 位	52-64 位	65-128 位

b) 类型域利用33 – 36位，共4比特，共有16种取值，用于标识城轨单位的不同类型的地址空间，地址空间类型宜根据生产类、管理类、服务类划分网络地址、终端地址、应用平台地址，剩余标识作为预留。地址类型划分宜参照表2。

表 2 地址类型标识划分

取值	地址类型说明	举例
0	安全生产类网络地址	FC00:0::0xxx:…
1	安全生产类平台地址	FC00:0::1xxx:…
2	安全生产类终端地址	FC00:0::2xxx:…
3	内部管理类网络地址	FC00:0::3xxx:…
4	内部管理类平台地址	FC00:0::4xxx:…
5	内部管理类终端地址	FC00:0::5xxx:…
6	外部服务类网络地址	FC00:0::6xxx:…
7	外部服务类平台地址	FC00:0::7xxx:…
8	外部服务类终端地址	FC00:0::8xxx:…
……	……	FC00:0::Xxxx:…
F	预留	FC00:0::fxxx:…

c) 机构域利用37－40位，共4比特，共有16种取值，用于标识总部、二级单位；统一管理定义城轨单位内各机构取值，该机构号码宜能唯一的标识出某一级单位、二级单位，以方便根据地址唯一快速的定位到具体某个单位。机构域标识划分宜参照表3。

表 3　机构域标识划分

取值	机构域说明	举例（以管理类终端为例）
0	集团总部	FC00:0::50xx:…
1	运营公司	FC00:0::51xx:…
2	建设公司	FC00:0::52xx:…
3	商业经营类公司	FC00:0::53xx:…
……	……	FC00:0::5Xxx:…
F	预留	FC00:0::5Fxx:…

d) 地域/部门域利用41-48位，共8比特，共有256种取值，可用于标识城轨单位各线路或者二级部门。如运营公司，考虑方便路由聚合和路由发布，其中地域字段取值宜按线路定义，0代表运营公司总部，其余表示按线路划分，多余的值预留。地域/部门域标识划分宜参照表4。其他子公司如不按照线路划分，可按分公司下属部门机构进行定义。

表 4　地域/部门域标识划分

取值	地域/部门域标识说明	举例（以运营公司管理类终端为例）
0	分公司总部	FC00:0::5100:…
1	1 号线	FC00:0::5101:…
2	2 号线	FC00:0:: 5102:…
3	3 号线	FC00:0:: 5103:…
……	……	FC00:0:: 510X:…
FF	预留	FC00:0:: 51FF:…

e) 专业域利用48～51位，共4比特，16种取值。可按照不同专业进行定义，如通信专业、票务专业、综合监控专业，以安全生产类终端进行自定义标识。专业域标识划分宜参照表5。

表 5　专业域标识划分

取值	说明	举例（以运营公司生产类终端1号线为例）
0	通信专业	FC00:0::2101:0…
1	票务专业	FC00:0::2101:1…
2	综合监控专业	FC00:0:: 2101:2…
3	信号专业	FC00:0:: 2101:3…
……	……	FC00:0:: 2101:X…
F	预留	FC00:0:: 2101:f…

f) 预留域使用48~64位，共16比特，预留字段后续可按照需求进行定义，或者按照各城轨单位申请固定前缀进行调整。

5.3　地址规划关键任务

地址规划过程中应开展以下活动：

a) 应对 IPv6 地址规划关键任务进行梳理，评估自身 IPv6 地址使用的内外环境和就绪程度；
b) 自顶向下梳理机构组织架构、网络结构；

c） 自顶向下梳理机构 IP 地址使用和分配情况；
d） 分析组织架构或区域划分（地域）、或层级模式（网络层级）的适配模式；
e） 制定机构 IPv6 地址总体规划及管理办法；
f） 基于 IPv6 特性的接入控制以及场景化 IPv6 特性运用；
g） 分发和管理 IPv6 网络前缀，分层级数据共享及交换；
h） IPv6 地址分配、接入方式、以及资产标识与追踪定位；
i） IPv6 地址全生命周期管理、回收及跟踪；
j） IPv6 地址空间管理、地址检测、追踪溯源；
k） IPv6 地址规划的调整及弹性冗余预留。

6 基础平台与支撑系统

6.1 一般要求

6.1.1 数据中心

数据中心分为 IPv4 数据中心和 IPv6 数据中心。IPv4 数据中心是基于 IPv4 物理网络构建；IPv6 数据中心是基于 IPv6 物理网络构建。IPv4 数据中心需要改造才能支持 IPv6；IPv6 数据中心原生支持 IPv6。数据中心建设应满足下列要求：

a） 现有数据中心可从 IPv4 over IPv4 向 IPv4/IPv6 over IPv4 演进，优先采用新建 IPv6 资源池区、地址转换技术或双栈改造技术实现基础设施改造；
b） 新建数据中心优先采用 IPv6 数据中心方案，数据中心物理网络全面使用 IPv6 单栈技术，支持端到端 IPv6 访问，且扩展支持 IPv4/IPv6 over IPv6，具备良好的兼容和演进能力。

6.1.2 IPv6 资源池和 IPv4 资源池互访

IPv6资源池和IPv4资源池互访流程见图1。

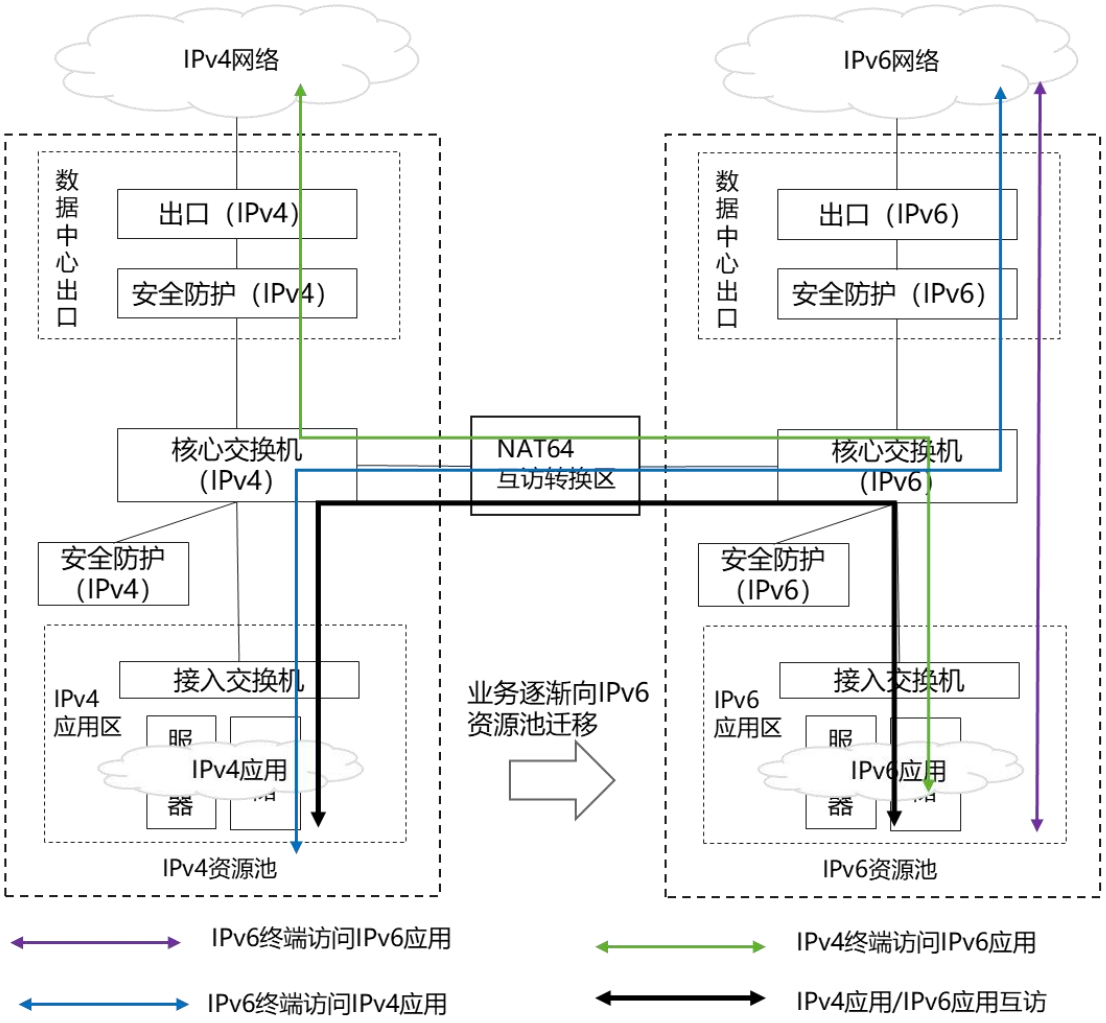

图 1　IPv6 资源池和 IPv4 资源池互访示意图

IPv6资源池和IPv4资源池互访有以下方式：

——IPv6 终端访问 IPv6 应用：IPv6 终端可访问 IPv6 资源池上部署的 IPv6 应用。IPv6 应用可获取终端真实的 IPv6 地址。

——IPv6 终端访问 IPv4 应用：IPv6 终端可通过 NAT64 访问存量 IPv4 应用。IPv6 流量经过 NAT64 后会转换成 IPv4 流量，IPv4 应用无法获取 IPv6 终端真实的 IPv6 地址，应在转换网关处实现映射溯源。

——IPv4 终端访问 IPv4 应用：IPv4 终端可访问存量的 IPv4 应用。

——IPv4 用户访问 IPv6 应用：IPv4 终端可通过 NAT64 访问 IPv6 应用。IPv4 流量经过 NAT46 后会转换成 IPv6 流量，在 NAT46 转换中，IPv4 源地址会嵌入 IPv6 的源地址中，IPv6 应用可通过 IPv6 源地址获取真实的 IPv4 地址。

——IPv4 应用向 IPv6 迁移：存量 IPv4 应用可先改造支持 IPv6，然后部署到 IPv6 资源池。这样同一个应用就有 IPv4 和 IPv6 两个部署实例。若两个部署实例涉及数据同步，可使用 NAT64 实现数据同步。

6.2　城轨云平台

6.2.1　IPv6 地址

城轨云平台IPv6地址应满足下列规定：

a)　云租户和云平台支持使用相同的地址前缀，通过标识位区分云租户和云平台；

b)　主机的IPv6地址支持通过DHCPv6或者SLAAC等方式自动获取，也可通过运维工具配置。

6.2.2 云平台

云平台应满足下列规定：

a) 云平台对外提供的接口支持 IPv6；
b) 云平台的内部通信支持 IPv6；
c) 云平台的管控和运维支持 IPv6。

6.2.3 租户 VPC

租户VPC应满足下列规定：

a) 租户VPC支持IPv6；

b) 租户VPC宜使用IPv6地址，默认不能被VPC外部的地址访问。若外部地址要访问VPC，需要配置相应的规则之后才能访问；

c) 租户VPC访问外部网络和云服务时，若流量从VPC发起，回程流量需要自动放通。若流量从VPC外发起，需要匹配相应的规则后才能访问VPC。

6.3 IPv6 支撑系统

6.3.1 DNS 系统

6.3.1.1 IPv6 地址支持

DNS系统IPv6地址支持应满足下列规定：

a) DNS服务器和解析器应完全支持IPv6地址记录（AAAA记录），以便在IPv6环境中正常解析域名；
b) 能够处理IPv6反向查询，即将IPv6地址转换为域名（PTR记录）。

6.3.1.2 协议兼容性

协议兼容性应满足下列规定：

a) DNS服务器和解析器应兼容IPv4和IPv6，能够在双栈环境中工作，确保无缝过渡；
b) 应遵循相关的IETF（互联网工程任务组）RFC标准，如RFC 3596（DNS扩展支持IPv6）、RFC 4472（IPv6操作指南）等。

6.3.1.3 安全性

安全性应满足下列规定：

a) 宜支持DNSSEC（DNS安全扩展），确保DNS数据的完整性和真实性，防止DNS欺骗和篡改；
b) 可采取访问控制、防火墙和入侵检测等安全措施，防止DNS服务器受到攻击；
c) 宜季度定期检查和修复潜在的DNS安全漏洞。

6.3.1.4 性能与可靠性

性能与可靠性应满足下列规定：

a) 单套DNS系统每秒宜支持不少于20万个域名解析请求，本地解析延时不高于10ms，提供高性能、低延迟的IPv6 DNS解析服务；
b) 宜支持负载均衡、冗余和故障切换等技术，提高DNS系统的可靠性和可用性；
c) 宜提供持续的性能监控和优化，保障IPv6增长需求。

6.3.1.5 管理和维护

管理与维护应满足下列规定：

a) 应提供IPv6 DNS管理工具和界面，以便进行地址分配、记录管理和配置；
b) 应制定清晰的DNS维护计划和流程，宜每周定期备份、月度更新和故障排查等计划和流程；
c) 应对DNS操作人员进行IPv6相关的培训和指导，提高其技能和能力。

6.3.2 DHCP 系统

6.3.2.1 IPv6 地址分配

IPv6地址分配应满足下列规定：

a) DHCP服务器应能够分配和管理IPv6地址，包括全局唯一地址和链路本地地址；
b) 支持前缀委派功能（Prefix Delegation），允许DHCP服务器为客户端路由器分配IPv6子网前缀。

6.3.2.2 协议兼容性

协议兼容性应满足下列规定：

a) DHCP服务器和客户端应兼容IPv4和IPv6，能够在双栈环境中工作，确保无缝过渡；
b) 遵循相关的IETF（互联网工程任务组）RFC文档，如RFC 3315（DHCPv6协议）、RFC 3633（IPv6前缀委派）等。

6.3.2.3 安全性

安全性应满足下列规定：

a) 支持安全的身份验证机制，宜使用安全的DHCPv6（Secure DHCPv6），防止未经授权的DHCP服务器分配地址；
b) 可采取访问控制、防火墙和入侵检测等安全措施，防止DHCP服务器受到攻击；
c) 宜季度定期检查和修复潜在的DHCP安全漏洞。

6.3.2.4 性能与可靠性

性能与可靠性应满足下列规定：

a) 单套DHCP系统宜支持每秒分配不少于1000个IP地址能力，提供高性能的IPv6 DHCP服务；
b) 宜支持负载均衡、冗余和故障切换等技术，提高DHCP系统的可靠性和可用性；
c) 宜支持持续的性能监控和优化，保障IPv6增长需求。

6.3.2.5 管理与维护

管理与维护应满足下列规定：

a) 应提供IPv6 DHCP管理工具和界面，以便进行地址分配、配置和监控；
b) 应制定清晰的DHCP维护计划和流程，宜每周定期备份、月度更新和故障排查等计划和流程；
c) 应对DHCP操作人员进行IPv6相关的培训和指导，提高其技能和能力。

6.3.3 IPAM 系统

6.3.3.1 IPv6 地址管理

IPv6地址管理应满足下列规定：

a) IPAM系统应能够支持IPv6地址的分配、回收和追踪；
b) 能够管理IPv6地址空间，包括全局唯一地址、链路本地地址和唯一本地地址；
c) 支持IPv6地址规划，包括地址分配策略、前缀长度和子网划分等。

6.3.3.2 协议兼容性

协议兼容性应满足下列规定：

a) IPAM系统应兼容IPv4和IPv6，能够在双栈环境中工作，确保无缝过渡；
b) 支持与其他网络协议和服务的集成，例如DHCPv6、DNSv6、路由协议等。

6.3.3.3 安全性

安全性应满足下列规定：

a) 提供安全的访问控制和身份验证机制，防止未经授权的访问和操作；
b) 可采取访问控制、防火墙和入侵检测等安全措施，防止IPAM系统受到攻击；
c) 宜季度定期检查和修复潜在的IPAM安全漏洞。

6.3.3.4 性能与可用性

性能与可用性应满足下列规定：

a） 单套IPAM系统宜支持管理不少于10万个终端地址，提供高性能的IPv6 地址管理服务；

b） 通过负载均衡、冗余和故障切换等手段，提高IPAM系统的可靠性和可用性；

c） 进行持续的性能监控和优化，确保满足不断增长的IPv6网络需求。

6.3.3.5 管理与维护

管理与维护应满足下列规定：

a） 应提供IPv6地址管理工具和界面，以便进行地址分配、配置和监控；

b） 应制定清晰的IPAM维护计划和流程，宜每周定期备份、月度更新和故障排查等计划和流程；

c） 应对IPAM操作人员进行IPv6相关的培训和指导，提高其技能和能力。

7 网络

7.1 一般要求

网络IPv6部署应满足下列规定：

a） 考虑到向IPv6单栈演进，在网络协议选择上选择SRv6协议作为网络互联互通协议，在终端和应用未全部完成IPv6改造时，业务侧应采用IPv4/IPv6双栈承载业务；

b） 根据生产、管理、服务等业务应用网络，优先在管理网络、服务网络进行IPv6部署，业务应用IP可采用IPv4或IPv6，网络采用IPv6单栈技术；

c） 生产网络优先在生产监控、数据采集业务应用进行IPv6部署，实时控制工业网络后续演进；

d） 具备条件的，可新建IPv6单栈网络，IPv4业务运行在原有网络，IPv6业务运行在新建网络；

e） IPv6改造适当考虑先进性，网络具备流量可调度、带宽确定性保障、故障快速发现及恢复、网络安全高效协同等能力，宜采用“IPv6+”技术；

f） 新建网络应支持telemetry技术，实现秒级网络状态感知；支持流量监测技术，实现城轨真实应用流量的带宽、时延、丢包率等采集，并支持流量回溯分析功能。

7.2 网络结构

城市轨道交通行业网络分为安全生产网、内部管理网、外部服务网，全面覆盖地铁各部门以及各条线路、车辆段、停车场等，应符合T-CAMET-11004以及T/CAMET11001规范。城市轨道交通IPv6网络整体架构如图2所示。

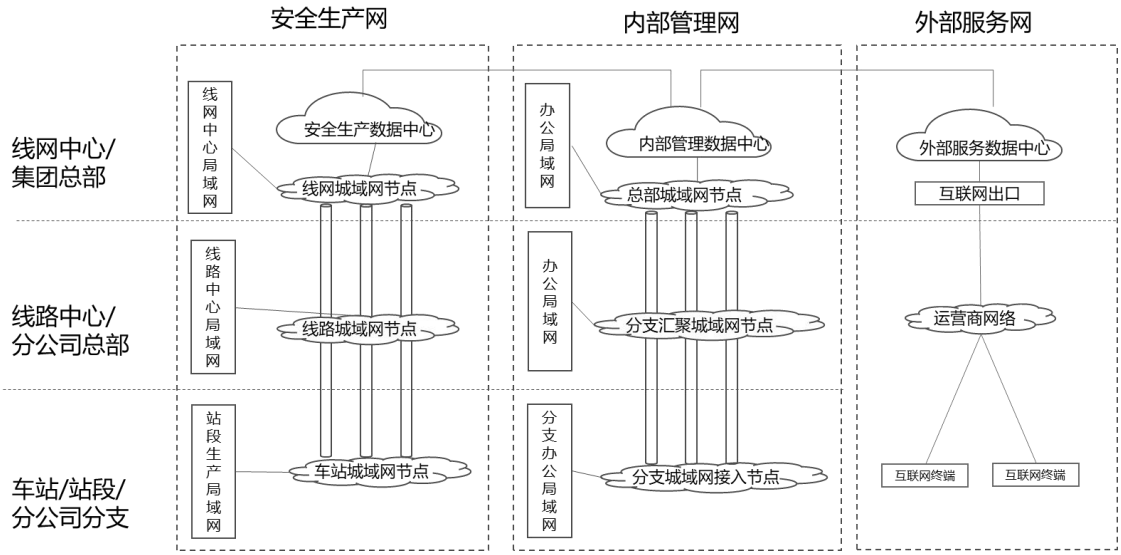

图 2 城市轨道交通 IPv6 网络整体架构

按照部署网络区域，划分为数据中心网络、城域网、局域网，如图3所示。

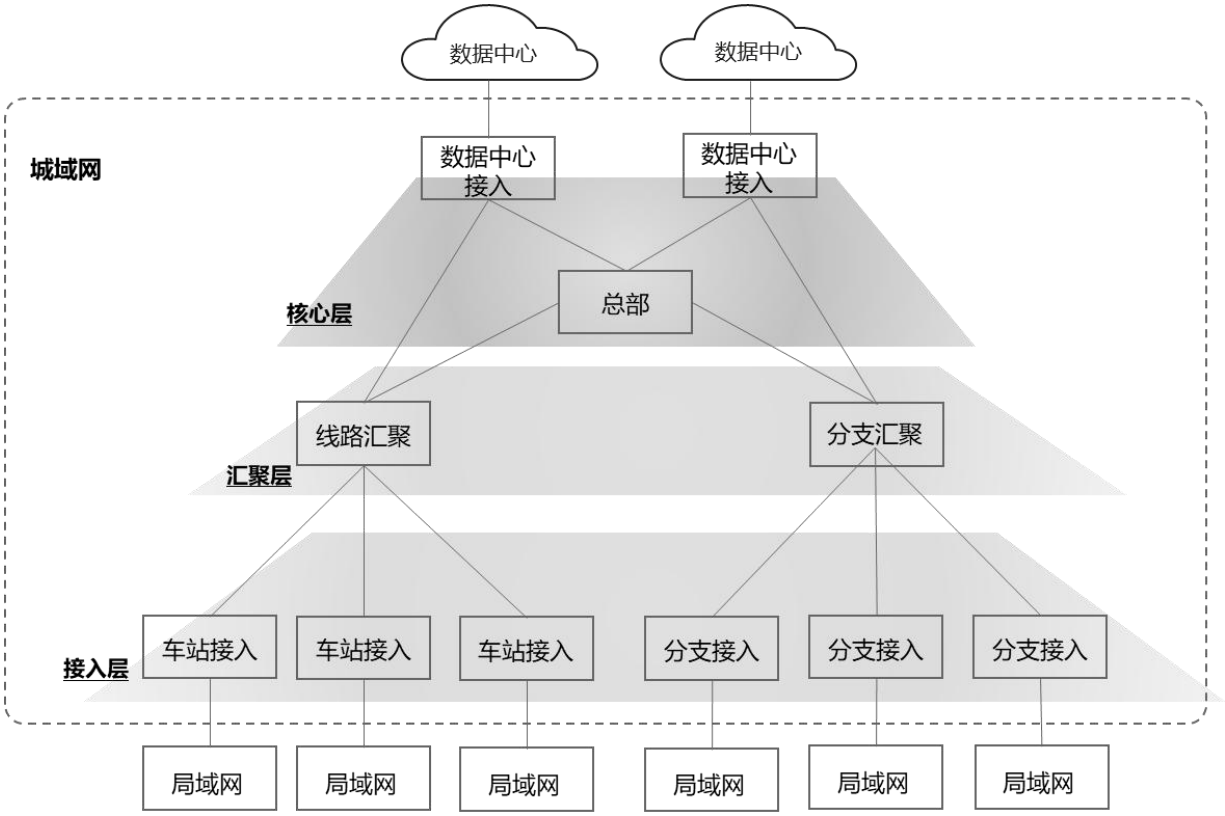

图 3　城市轨道交通 IPv6 网络部署图

7.3　城域网

7.3.1　网络组成

城域网由城轨传输链路和各级网络节点设备组成，分级建设、分域管理。宜分为核心、汇聚、接入三级网络架构，部分城市按需可分为核心和接入两层架构。三级网络架构如图4所示，包含以下内容：

a）　核心层：主要为城轨集团总部，主备数据中心等节点，主要包括部署位置在主要的数据中心互联，提供汇接多个接入设备或汇聚设备的能力；

b）　汇聚层：主要为线路控制中心或分支总部等节点，主要用来汇聚连接到核心层的网络的流量，分为线路中心汇聚和分支汇聚。线路中心汇聚主要是指线路中心的流量，分支汇聚主要指办公分支汇聚节点；

c）　接入层：主要是各个车站、车辆段和分支办公室，提供站段局域网接入。

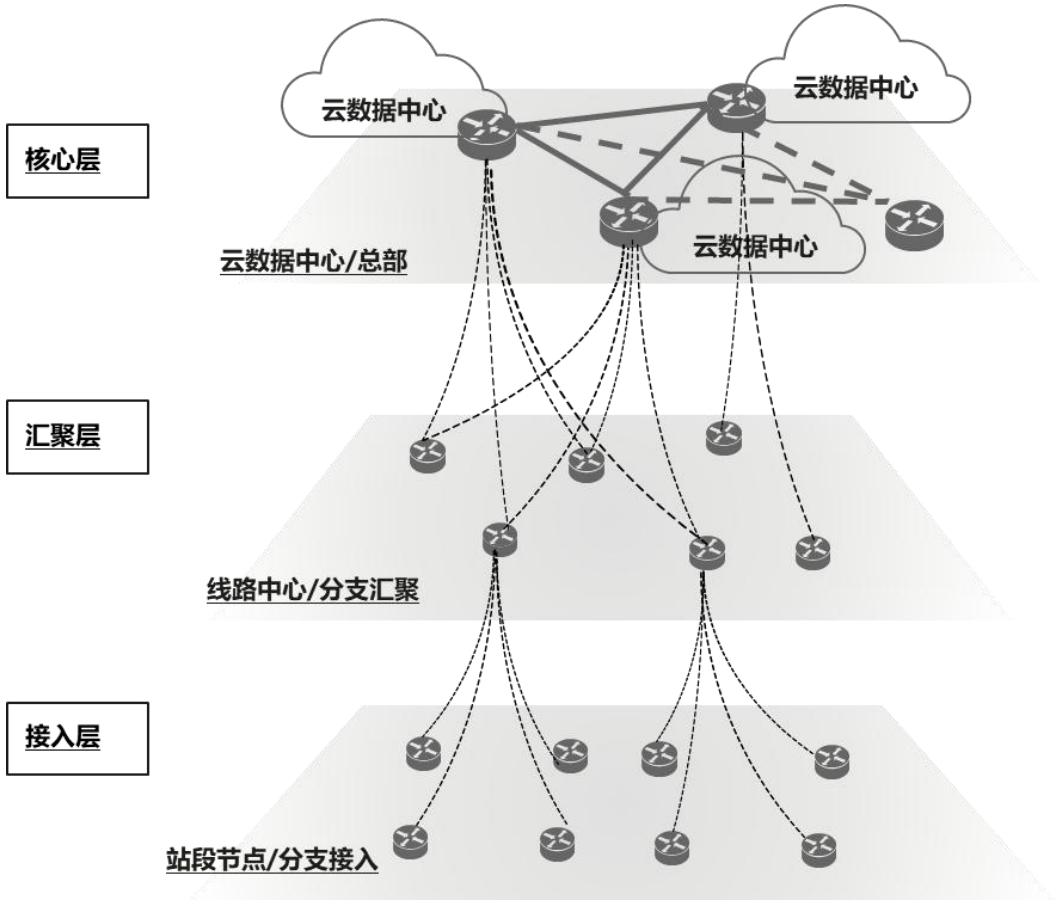

图 4　城域网的三级网络架构

7.3.2　网络部署

城域网络的IPv6部署应满足下列规定：

a)　城域网应支持IPv4/IPv6双栈，宜采用IPv6单栈建设部署；

b)　宜在城轨云中心与车站边缘节点接入网络采用IPv6+技术，新建或整网改造的城域网应采用Segment-Routing IPv6（IPv6 分段路由）的 SDN 技术，符合 IETF RFC 8754 等要求，SDN网络服务宜支持多策略选路、路由精确控制、流量全局调度等功能；

c)　应支持业务流量进行动态调整，实现城域网链路的负载均衡，避免流量走单边，提升链路利用率；

d)　应对网络中业务运行状态、服务质量进行实时监控，主动运维，宜采用大数据技术及iFIT随流检测技术；

e)　安全生产网宜根据专业应用划分通信、信号、综合监控、自动售检票等业务分片，宜采用Flex Ethernet技术实现网络切片；

f)　内部管理网络宜根据业务系统划分为运营管理、企业管理、建设管理、资源管理等业务分片，宜采用Flex Ethernet技术实现网络切片。

7.3.3　自治域

7.3.3.1　IPv6 网络自治域规划宜采用单独一个自治域。单个网络自治域内不宜超过 1000 台网络节点设备。

7.3.3.2　自治域号码

IPv6自治域号码独立分配和管理，具体分配和管理原则应满足下列规定：

a)　自治域号码由管理中心统一分配和管理；

b) 内部采用私用自治域号码，按照层次性和连续性的原则进行分配；
c) 内部自治域号码不允许重复；
d) 私有自治域号码仅在内部出现，不传递给其他网络。

7.3.4 路由

7.3.4.1 路由协议

IPv6路由协议应满足下列要求：
a) 自治域内的路由发现和通告可采用静态路由或动态路由协议，采用动态路由协议时宜采用IS-ISv6。

7.3.4.2 路由策略

IPv6路由策略应满足下列规定：
a) 应实现承载网路由和用户路由分离，避免用户网络的业务路由的振荡影响承载网路由；
b) 承载网路由宜采用IS-ISv6承载，包括承载网设备互联地址路由、Loopback地址路由、SRv6 Locator地址路由等；
c) 用户路由宜采用BGP4+承载，包括用户业务地址路由、数据中心业务地址路由等；
d) 应合理规划IGP区域，控制路由规模，当网络规模较大时，应将IGP划分多个区域或多个进程。如城轨云数据中心、城域网和局域网等区域。

7.3.4.3 路由通告

IPv6路由通告应满足下列规定：
a) 用户路由通过MP-BGP协议在自治域内通告，也可使用静态路由与上级网络对接；用户路由通告前应进行聚合；
b) 承载网路由通过IGP协议在自治域内通告。

7.3.5 VPN 业务部署

采用隧道和VPN作为统一的多业务平台承载技术，IPv6业务宜提供VPN承载能力，并满足下列规定：
a) 针对不同的业务或者接入单位在对应的网络设备创建VPN实例，满足不同IPv6业务承载需要；
b) VPN业务宜使用隧道技术进行承载,存量网络可采用基于MPLS的6VPE技术,有条件的可采用SRv6技术，新建网络宜采用SRv6技术。

7.3.6 服务质量

网络服务质量应符合下列规定：
a) 网络宜具备在链路故障或IPv4/IPv6双栈业务质量恶化时快速感知并调整到质优链路的能力；
b) 应能为IPv4/IPv6重点业务提供确定性带宽保障，宜采用专用设备和物理链路承载或网络切片技术，例如视频监控、行车安全监控、办公业务等；
c) 应具备在网络故障或IPv4/IPv6双栈业务服务质量恶化时快速故障定位能力，宜采用iFIT随流检测技术。

7.4 局域网

7.4.1 网络组成

站段、分支局域网物理网络宜采用以核心层为根的树形网络结构，宜采用核心层、汇聚层、接入层三层结构（如图所示），对于规模较小的分支单位部门，可采用核心层、接入层两层结构。局域网物理网络结构如图5所示。

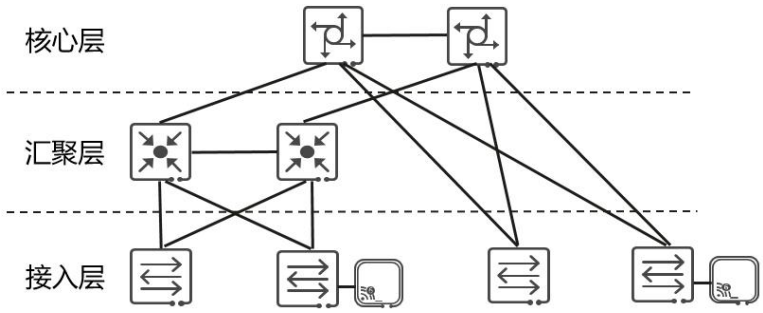

图 5　局域网物理网络结构

7.4.2　IPv6 部署

局域网IPv6部署应满足下列规定：

a）　局域网内应确保网络传输过程中IPv6数据包的源、目的地址不发生改变，不宜部署NAT转换；
b）　有线终端可采用DHCPv6、SLAAC方式分配IPv6地址，DHCPv6方案宜采用集中服务器方式，网络部署DHCPv6 Relay，中继DHCPv6相关报文；
c）　无线接入终端存在多样性，宜采用无状态的地址获取方案SLAAC混合方案分配IPv6地址；
d）　无线控制器作为认证点宜支持IPv6 Radius报文；
e）　无线接入点AP管理IP地址，宜通过无线控制器配置DHCPv6或者SLAAC为AP分配地址；
f）　访问外部网络的终端，宜开启SLAAC隐私扩展功能，启用临时IPv6地址，并提供安全溯源、策略联动方案；
g）　安全生产网终端宜采用DHCPv6 EUI64方式为专业终端分配IPv6地址，实现终端的MAC地址和IPv6地址强绑定；
h）　宜采用VxLAN IPv6、Flex Channel等技术，对局域网不同业务终端进行安全隔离。

7.4.3　网络技术

网络技术应满足如下规定：

a）　宜在运维管理区部署DHCPv6服务器，为终端统一分配IPv6地址；
b）　终端的IPv6三层网关可集中部署在核心交换机，或分布式部署在接入交换机上；
c）　应在三层网关部署DHCPv6 Relay，由DHCPv6服务器为终端统一分配IPv6地址；对于存在安卓终端接入的部门，应同时在三层网关部署SLAAC，为安卓终端分配IPv6地址；
d）　二层网络应支持DHCPv6 Snooping，防止非法DHCPv6服务器攻击；应支持ND Snooping，防止非法RA攻击；宜支持MLD Snooping，避免IPv6二层组播流量泛洪；
e）　接入设备作为终端接入认证点，应支持IPv6场景下的802.1x/Portal/MAC认证；

7.4.4　网络运维管理

网络运维管理应满足如下规定：

a）　应支持IPv6地址的管理，对地址的分配情况、使用情况等进行直观展现；
b）　应支持IPv6接入认证、地址获取等的协议回放，满足故障情况下的快速定位；
c）　应支持对网络设备的FIBv6、ND等IPv6资源进行监控，预警资源超限风险。

8　安全

8.1　一般要求

城市轨道交通行业安全生产网、内部管理网、外部服务网和运维管理网内的主要应用系统可参考T/CAMET 11005进行等级保护级别参考，应用系统通用安全参考GB/T 22239-2019中相关部分及本章节内容做优化完善。

8.2　IPv6 等级保护要求

8.2.1　安全通信网络

8.2.1.1 网络架构

网络架构应满足下列规定：

a) 宜优化IPv6网络设计，避免双栈机制带来的复杂度和潜在风险，确保网络的高效性和安全性；
b) 可启动IPv6单栈试点项目，选取非核心业务区域，实施IPv6单栈网络试验，积累实战经验，为全面转型做铺垫；
c) 宜对网络中业务流量进行监控、安全分析和威胁溯源，联动网络设备执行威胁隔离动作，避免不同业务安全威胁扩散。

8.2.1.2 通信传输

通信传输应满足下列规定：

a) 应实现IPv6通信的加密传输，利用IPsec提供端到端的加密和认证，增强通信的安全性；
b) 等级保护三级网络应配置IPv6的流量监控和过滤机制，防止未授权访问和恶意流量；
c) 等级保护三级网络宜采用先进的加密算法和协议，确保IPv6通信的机密性和完整性。

8.2.2 安全区域边界

8.2.2.1 边界防护

边界防护应满足下列规定：

a) 应部署支持IPv6的边界防护设备，如防火墙，过滤IPV6非法地址和异常报文头，防止未授权访问；
b) 应对IPv6地址进行管理和分配，确保地址的合法性和唯一性，防止地址欺骗；
c) 等级保护三级网络应定期更新防火墙规则，以适应IPv6网络中可能出现的新威胁；
d) 对终端应进行准入控制，对仿冒，私接、流量异常等行为应进行检测、识别和阻断；
e) 宜评估和测试新型边界防护技术，以提升IPv6网络边界的安全防护能力。

8.2.2.2 访问控制

访问控制满足下列规定：

a) 应实施IPv6访问控制列表，控制对网络资源的访问权限；
b) 宜月度审查和更新访问控制列表，确保其适应IPv6环境下的安全需求；
c) 可采用动态访问控制机制，根据网络状况自动调整访问策略。

8.2.2.3 入侵防范

入侵防范应满足下列规定：

a) 应部署支持IPv6的入侵检测系统（IDS）和入侵防御系统（IPS），检测并阻止针对IPv6网络的攻击；
b) 等级保护三级网络宜利用IPv6的流标签等特性，优化入侵检测系统的性能和准确性；
c) 等级保护三级网络宜整合IPv6威胁情报，提高入侵检测系统的准确性和响应速度；
d) 可接入实时威胁情报源，增强系统对新兴IPv6威胁的识别与响应能力。

8.2.2.4 安全审计

安全审计应满足下列规定：

a) 应实施全方位、多层次的安全审计机制，确保全面记录和跟踪IPv6通信环境中的所有安全相关事件及系统、用户的操作行为；
b) 应为IPv6环境下的安全审计制定专门的审计策略和流程；
c) 宜采用集中化的日志管理系统，便于事件的关联分析和合规审查；
d) 可建立基于大数据分析的安全审计系统，实现日志的深度挖掘和智能分析，提升审计效能。

8.2.3 安全计算环境

8.2.3.1 身份鉴别

身份鉴别应满足下列规定：

a) 应实施强身份认证机制，确保IPv6网络中用户身份的准确性、真实性和可靠性；
b) 等级保护三级网络宜采用多因素认证，提高身份鉴别的安全级别；
c) 可选取特定部门或关键岗位，实施生物特征识别作为辅助身份验证手段，增强认证安全性。

8.2.3.2 入侵防范

入侵防范应满足下列规定：
a) 应部署终端安全管理和防护软件，监测并阻止针对IPv6主机的攻击；
b) 等级保护三级网络宜月度对终端进行漏洞扫描和补丁管理，减少被IPv6相关漏洞攻击的风险；
c) 宜采用基于IPv6的零信任网络架构，在部分业务域内试用零信任安全框架，实现基于身份和上下文的动态访问控制，优化安全策略。

8.2.3.3 访问控制

访问控制应满足下列规定：
a) 应实施基于IPv6地址的细粒度访问控制策略，确保资源的安全访问；
b) 等级保护三级网络宜考虑IPv6的特定应用场景（如物联网），制定针对性的访问控制策略；
c) 等级保护三级网络宜采用IPv6微分段技术，进一步细化访问控制，提高安全性。

8.2.3.4 网络保护与恢复

网络保护与恢复应满足下列规定：
a) 应制定并实施网络保护和恢复策略，确保在IPv6环境下遭受攻击时能够迅速恢复服务；
b) 等级保护三级网络宜定期进行网络应急演练，检验网络保护和恢复策略的有效性；
c) 等级保护三级网络宜建立灾难恢复中心，提供异地备份和快速恢复能力；
d) 可部署云原生的备份与恢复系统，增强灾备方案的弹性和便捷性。

8.2.4 安全管理中心

8.2.4.1 集中管控

集中管控应满足下列规定：
a) 等级保护三级网络应建立支持IPv6的安全管理中心，实现对IPv6环境下网络架构、通信传输、区域边界和计算环境的集中管控；
b) 应制定统一的安全管理策略，确保IPv6和IPv4环境下的安全管理一致性和协调性；
c) 等级保护三级网络宜利用IPv6的特性和优势，优化安全管理中心的性能和功能；
d) 等级保护三级网络宜采用自动化运维工具，减少人为错误，提高安全管理的效率；
e) 等级保护三级网络可引入AI与机器学习技术，实现安全策略智能优化与自动化威胁预测；
f) 可开发或采用基于IPv6的远程监控与管理系统，提升网络运维效率与管理灵活性。

8.3 密码要求

8.3.1 密码技术

使用的密码技术应满足下列规定：
a) 所有基于IPv6的网络设备、安全产品和服务平台应支持国家商用密码算法（如SM系列算法），确保通信过程中的数据加密、身份认证符合国家密码管理规定；
b) IPv6系统中使用的密码模块应通过国家商用密码检测认证，确保密码技术的安全性和合规性；
c) 宜在IPv6协议栈中集成国密版的IPSec等协议，以提高数据传输的安全性和兼容性；
d) 宜建立完善的国密密钥管理体系，包括密钥的生成、分发、存储、更新及销毁，宜采用自动化管理工具提升效率和安全性；
e) 考虑到国密算法可能对系统资源的消耗，可根据实际情况优化算法实现，提高IPv6环境下国密应用的性能。

8.3.2 密码应用安全性评估

密码应用安全性评估应满足下列规定：

a) 所有涉及IPv6的网络设施和信息系统应定期进行密码应用安全性评估，确保密码技术的有效性和安全性符合国家要求；
b) 针对密评中发现的问题，应制定整改计划并按时完成整改，确保安全隐患得到及时消除；
c) 在IPv6部署前，宜进行密码应用的风险评估，识别潜在安全威胁，为后续的密评提供参考；
d) 宜定期对技术人员进行密码学和IPv6安全相关的培训，增强整个组织的密码安全意识；
e) 可引入第三方专业机构进行深度密码应用安全审计，以获得更全面、客观的安全评估结果。

8.4 数据安全

数据安全应满足下列规定：
a) 在IPv6环境中，所有数据应根据敏感程度进行分类，并实施相应级别的保护措施；
b) 应实施严格的访问控制策略，确保只有授权用户和系统能访问敏感数据；
c) 宜使用国密算法对IPv6网络中传输的数据进行加密，特别是在跨越不安全网络时，确保数据的机密性；
d) 宜建立完善的数据操作日志系统，记录并定期审计IPv6环境下的数据访问和操作行为，便于追踪异常活动；
e) 可实行数据生命周期管理策略，包括数据的创建、使用、存储、归档及销毁等环节，提升数据管理效率和安全性。

9 应用

9.1 一般要求

9.1.1 业务系统 IPv6 适配

业务系统IPv6适配应满足下列规定：
a) 现有的业务系统，采用双栈技术或翻译技术，实现终端的双栈访问；
b) 新建线路及升级改造的业务系统优先采用IPv6单栈模式，支持双栈终端访问；
c) 针对城市轨道新型业务系统应用，优先采用APN6创新技术；优先在终端和应用嵌入APN应用标签，在IPv6+网络中识别用户终端访问的应用需求，提供精细的网络服务能力。

9.1.2 B/S 应用技术要求

门户网站属于B/S架构，应用IPv6适配应满足下列规定：
a) 通过双栈技术或翻译技术,实现支持 IPv4 和 IPv6 双栈访问;其次在网站域名的权威 DNS 服务器上添加域名的AAAA 解析，实现 IPv6 终端的域名解析；
b) 双栈代码改造，应使用兼容 IPv4 和 IPv6 的 API 或 SDK，对代码中的 URL 和 URI 链接，应采用域名的方式编写；数据库、 溯源日志存储的IP字段，代码中使用的IP数据结构，应兼容 IPv4 和 IPv6 地址长度;应采用支持 IPv6 常用操作系统版本、数据库版本和中间件版本。

9.1.3 C/S 应用技术要求

生产信息化系统，可分为C/S和B/S架构。采用C/S架构应用IPv6适配应满足下列规定：
a) 客户端采用双栈代码改造方式，实现对 IPv4 和 IPv6 双栈的支持；
b) 服务器端程序，若业务功能简单，宜采用双栈技术对代码进行改造；若业务功能复杂，采用翻译技术，实现对 IPv6 的支持，并逐步进行系统改造，最终实现端到端的 IPv6 升级。

9.2 业务应用

9.2.1 生产类应用

生产类应用应满足下列规定：
a) 城域网采用灵活以太Flex Ethenet网络切片，传输网宜采用比特透传模式对接；
b) 乘客信息、视频监控业务采用组播方式时宜采用PIMv6或Bierv6技术；
c) 乘客信息系统采用C/S、B/S结合的软件架构，宜采用SQL SERVER、Oracle等支持IPv6协议栈的数据库版本，宜采用Tomcat等支持IPv6协议栈的中间件；

d) 综合监控系统可兼容 IPv6 标准协议，应支持采用不同厂商的 IPv6 终端设备、网络设备和网络安全设备；
e) 综合监控系统与BAS、PSCADA深度集成，宜采用相同的IPv6网络协议标准；
f) 综合监控业务终端宜支持 IPv4/IPv6 协议翻译技术，可在 IPv4 和 IPv6 网络间进行通信；
g) 综合监控应用终端宜采用手动分配固定 IPv6 地址，采用冗余 A、B 网架构时，应支持不同子网地址标识；
h) 综合监控系统在IPv6应用环境下，应保证控制命令响应时间小于2秒，设备状态变化信息响应时间小于2秒，单站实时数据画面在工作站整体整幅调看响应时间应小于1秒；
i) LTE-M基站宜采用IPv6网络承载，网络应支持1588v2时钟协议；
j) 5G网络承载宽带集群、车载乘客信息系统、车载视频监控等多业务时，宜采用网络切片技术，满足YD/T 3975-2021 《5G网络切片 基于IP承载的端到端切片对接技术要求》。

9.2.2 管理类应用

管理类应用应满足下列规定：
a) 视频会议应用宜采用APN6 技术，根据应用携带的信息自动选择网络和安全服务；
b) 视频会议系统、IP电话系统采用H.232、SIP协议等多媒体协议方式，宜采用双栈技术或NAT应用层网关方式；
c) 针对BIM应用等突发大带宽业务，宜采用APN6技术，根据应用携带信息动态调整数据包传输。

9.2.3 乘客服务类应用

乘客服务类应用应满足下列规定：
a) 门户网站应用、乘客服务、互联网售检票等APP应用应支持IPv6终端访问，宜支持IPv6 域名DNS服务；
b) 门户网站应用宜支持IPSecv6安全协议，保证访问的安全性，并防控重放攻击；
c) 乘客服务应用宜支持APN6及网络切片功能，根据用户需求负载动态调整数据包传输；
d) 互联网售检票应用宜利用IPv6扩展报头实现IPSec安全加密，保证数据传输的安全性；
e) 互联网售检票应用宜采用网络切片技术，建立独立虚拟专网保障敏感数据安全。

9.3 应用演进路线

9.3.1 新建工程

新建工程应满足下列规定：
a) 新建工程涉及的平台系统及IP设备终端应按IPv6标准建设，且支持IPv4/IPv6 双栈访问；
b) 考虑新建线路与既有线网系统的兼容性，初期新建线路应采用IPv4/IPv6双栈，逐渐向IPv6单栈演变。

9.3.2 改造工程

改造工程应满足下列规定：
a) 改造工程涉及的平台系统及IP设备终端应按IPv6建设，当既有设备系统主要为IPv4单栈时，新购设备宜采用IPv4/IPv6双栈；
b) 改造后的平台系统应支持IPv4终端设备的接入及功能实现；
c) 改造后的平台系统应支持与IPv4平台系统的互联互通；
d) 改造后的平台系统及IP设备终端应至少满足改造前的原有功能；
e) 改造后的平台系统及IP设备终端应不影响换乘站原有的互联互通功能。

10 终端

10.1 一般要求

终端IPv6部署应满足下列规定：
a) 充分考虑IPv6地址的分配、管理、监控、溯源，确保故障的快速处理和安全事件的精准溯源；

b） 在IPv4/IPv6双栈模式下，优先使用IPv6方式进行通信。

10.2 终端要求

10.2.1 计算机终端

计算机终端应满足下列规定：

a） 应支持通过DHCPv6方式获取IPv6地址；
b） 应建立计算机终端接入网络的审批制度；
c） 应根据各内设部门的工作职能和处理业务的重要程度，划分不同的子网，并制定各子网间的访问规则和策略；
d） 应制定对计算机终端在网络上的统一命名规则，名称应易于识别；
e） 应设置并启用网络接入控制策略，通过实名接入认证、限制物理接入点、IP地址与MAC地址绑定等措施，将接入的计算机终端限定在指定的物理子网或逻辑子网中；
f） 应支持IPv6场景下的802.1x或Portal方式进行网络准入认证；
g） 应限制远程接入的计算机终端数量、接入方式、访问范围等。

10.2.2 移动智能终端

移动智能终端应满足下列规定：

a） 应支持通过DHCPv6或SLAAC方式获取IPv6地址；
b） 应支持IPv6场景下的802.1x或Portal方式进行网络准入认证；
c） 应使用安全加密方式接入无线网络，宜采用WPA3加密方式。

10.2.3 物联终端

物联终端应满足下列规定：

a） 应支持通过DHCPv6或SLAAC方式获取IPv6地址；
b） 应支持IPv6场景下的802.1x或Portal方式进行网络准入认证；
c） 应使用安全加密方式接入无线网络，宜采用WPA3加密方式；
d） 宜支持将机电设备大量IO点位的物联设备转无线设备，接入无线网络。

10.2.4 哑终端

哑终端应满足下列规定：

a） 应支持通过DHCPv6方式获取IPv6地址；
b） 应支持MAC认证方式进行网络准入认证。